PX194

From: [redacted]
Sent: 1/15/2018 8:09:38 PM
To: [redacted]
Subject: Fwd: thinking on telegram

How did your meeting with Pavel go?

Sent from my iPad

Begin forwarded message:

From: [redacted]
Date: January 13, 2018 at 1:18:04 AM PST
To: [redacted]
CC: [redacted]
Subject: Re: thinking on telegram

100% agree

I do not find our criticisms hyperbolic. My reasons boil down to:

1) They roll their own crypto and can't even get a chat app's crypto right let alone an economic protocol's

2) Hypercube scaling doesn't work according to Vitalik and he found this out 4 years ago. Raising billions and being so unaware of what's going on is pretty crazy

3) The paper mentions 2^92 child blockchains, which is literally more than the number of computers that exist on the planet

I'd need very good answers to all 3 of those, they're all super fair game, and if this were the Pope's deal I'd still be asking the same 3 questions. Might be a decent trade, but the price is high and I'm not bullish on it as a long term investment until they have decent answers to these questions so I'm a pass until then

Regards,

[redacted]
CO-CHIEF INVESTMENT OFFICER

[redacted]

On Sat, Jan 13, 2018 at 12:39 AM -0800, [redacted]:

I'm cc'ing [redacted] here because I don't think [redacted] or I have ever shared our concerns beyond hyperbolic criticism.

On the profoundly credible technologists, I actually disagree with that. Telegram is a cool app that I enjoy using but is neither as secure nor as trusted as Signal. See the below quote by an actual expert:

"They use the MTproto protocol which is effectively homegrown and I've seen no proper proofs of its security," Alan Woodward, professor at the University of Surrey. Woodward criticized Telegram for their lack of transparency regarding their home cooked encryption protocol. "At present we don't know enough to know if it's secure or insecure. That's the trouble with security by obscurity. It's usual for cryptographers to reveal the algorithms completely, but here we are in the dark. Unless you have considerable experience, you shouldn't write your own crypto. No one really understands why they did that."

This is the Telegram approach to doing things. It is incompatible with blockchain technology; the Bitcoin whitepaper gives a clear enough specification of how it will work that any well enough informed researcher could validate the core ideas. The stuff that does go unsaid has introduced massive headaches;

the blocksize is one such example, the necessity of SegWit, etc. All of those issues cropped up from pure implementation details. You *cannot* mess up something decentralized in a fundamental way; anything less than absolute correctness is absolute failure. Even though Bitcoin is *fundamentally perfect*, there are enough implementation issues that everyone is still arguing about how best to fix them, and whether hard forking to fix them will destroy the ability for anyone to trust it. Think about whether you would sell your Ether if I told you right now that there existed a deep fundamental flaw that would require a breaking hard fork to fix. Not an improvement we knew with high confidence would help scale or otherwise improve the network, one that would be required to keep it from completely failing.

Ton's 132 page whitepaper says nothing substantial about the hard parts of designing a decentralized protocol. It is essentially a wishlist of things they want to have, and how it will work assuming that their wishlist doesn't crash and burn. It does not make any substantial contributions to proof of stake research. It does not make any substantial contributions to sharding research. It does not make any substantial contributions to "hypercube routing" research. It does not say anything about why they will be able to do things Vitalik cannot, and it is insane to say it's because he can't hard fork Ethereum. He already has, many times, and there are many more hard forks planned to change fundamental properties of the Ethereum network. But all of those changes are discussed, debated, and if disproven abandoned. In 132 pages they've managed to summarize the state of current blockchain research and make no *provable* claims about its future.

The last point is why we don't like TON. I do not know how it will work. I cannot, in 132 pages, gain the slightest intuition as to how to go about proving that the hard problems it needs to solve will be solved. It's not just that it isn't a bulletproof specification; I don't even know how to begin evaluating if it will work at all. I might throw house money into this with no lockup and at a lower valuation. I probably wouldn't even throw house money into this under the actual lockup and valuation, but I still might. I certainly would not put a single cent I care more than nil about losing into this.

Mostly, because I think that this is an opportunistic ploy. Holding a sale while disallowing the release of the technical whitepaper restricts the class of people able to evaluate it to those that are both technically able to and also able to invest. That is almost the null set. It is antithetical to the entire philosophy of the space, and the actual terms of the raise are similar to selling a massively out of the money call option on a biotech that promises a drug to cure cancer without allowing anyone but investors to see the underlying research, 99.9999% of whom are not equipped to evaluate it. It's peer review by venture capitalist.

All of that being said, obviously it is your decision. I just wanted to be sure we didn't leave you only with hyperbolic criticisms.

Best,
[redacted]

On 1/12/18, 5:54 PM, [redacted] wrote:

> Sent from my iPhone
>
> Begin forwarded message:
>
> From: [redacted]>
> Date: January 12, 2018 at 5:46:59 PM PST
> To: [redacted]>
> Cc: [redacted]
> Subject: Re: thinking on telegram
>
> Understood.
>
> On Jan 12, 2018, at 3:39 PM, [redacted]> wrote:
>
> I'm with Pavel tomorrow afternoon and am exploring the second question. On the first it's a leap but with profoundly credible technologists. He's 5x oversubscribed at 600m so we have little to no leverage. Happy to chat when I'm back Sunday
>
> On Jan 12, 2018, at 6:32 PM, [redacted] > wrote:
>
> Guys, what do you think?
>
> From: [redacted]
> Sent: Friday, January 12, 2018 8:32 AM
> To: [redacted]

Subject: RE: thinking on telegram

[redacted] Do you think we could do a call with [redacted] to figure out how [redacted] got comfortable on the technology? The things I worry about on this are two fold (a) the technology- I didn't think he really answered the question around ETH/Vitalik- saying that ETH couldn't do it b/c it would be too hard to get consensus doesn't make sense given the "benevolent dictator" seems to be pretty good at getting his development community to pivot (b) the size of the raise (sounds like it will definitely be more than $600mm and a bunch is for Pavel to take off table for past investment)- I worry at a $3bn EV, where can this really go near term from upside? The reason ICON worked so well (and WAX) is they start at such a low EV. Law of large #s makes this one harder to work to the up, but to the down it has the same downside

From: [redacted]
Sent: Thursday, January 11, 2018 7:33 AM
To: [redacted]
Subject: FW: thinking on telegram

Just sharing this Telegram ICO color from a friend at a VC firm who has already heard their pitch:

Begin forwarded message:
Bull Case

* BTC and ETH have important flaws that prevent mainstream consumer adoption -mostly around scalability and usability
* Opportunity to build a new blockchain platform with a scalable currency and associated distributed services - in some sense a "better Ethereum" - is massive - ETH, which is only 2 years old, technically immature, and has very little non-speculative engagement, has a market cap of $120B. If TON can get meaningful consumer adoption and engagement across its services, and the macro market holds up, it could be worth $100B++.
* Telegram is a unique property to deliver on this vision

* 200M DAU bootstraps GRAM and their decentralized services - telegram instantly becomes largest crypto wallet
* Telegram is where deep crypto engagement happens today. Could be best on-ramp for next generation of crypto entrepreneurs building projects on top of TON.

* Team is uniquely strong and has an ethos of "for the people, by the people" - Success with Vk and Telegram speaks for itself. Importantly, the libertarian ethos that the Durov brothers have is of the nature you want to back in a decentralized ambition like this.
* Presale economics are fundamentally attractive - 50-80% discount with lock ups beginning to expire in 3 months is more attractive than the other high quality ICOs we've looked at. If desired, we likely could recoup principal given this discount and lock up expiry (assuming macro mostly holds).

* Questions / Risks

* Valuation and macro - Hard to connect all of the above to valuation which will be an imputed market cap that will be in the billions. Lots of dependency on macro market. There will be an altcoin collapse. Wonder whether we're in 1997 or 1999.
* Focus too broad - Their ambition is to build the decentralized web and all of its associated services. Its not small. Coupled with team size and amount of capital they'll raise, worry they'll dilute themselves and be unable to deliver on such a wide mandate.
* Competition - There are projects that are far ahead in each of the areas TON wants to build - distributed storage (filecoin, sia), proxies (mesh), dns (blockstack). Telegram will have bootstrapped distribution advantage, but will be behind on product and potentially in getting to market. Further, if Google or Facebook wanted to build something like this, they could probably blow Telegram out of the water and have much larger user bases to leverage.
* Team is not deep in crypto, and is small - Will they be able to hire crypto experts to solve some of the technical approaches they detail like infinite sharding? What are the downsides to these scaling solutions? Can they grow from 15 developers quickly before a much larger company decides to do something similar?
* Headline risk - There's a fair amount of illicit activity orchestrated through telegram. Possible TON could assist/further enable that. I do think the risk here is diffused given the breadth of institutional investors that will participate

Market data:

* VC firms taking allocations (non exhaustive, believe these are all non-binding)

* [redacted] - largest check for 50-100M+
* [redacted] coming in for 20M
* [redacted] coming in for a few million
* [redacted] coming in- not sure $
* [redacted] coming in - not sure $
* Almost all of the notable crypto funds are coming in - not sure $

* Other market data
    * ~10 key Russian families with interest totaling >600M
    * Some people close to Telegram folks think that everyones allocations are going to be cut by ~50% given expected demand
    * $2B in demand so far without having gone to China
    * Worth noting [redacted] / [redacted] / [redacted] - who are viewed as smart crypto pickers to date - do not look like they are participating

Sent via [redacted]